Version Number: 01-2019

U.S. Department of Commerce
National Oceanic and Atmospheric Administration
National Weather Service

Privacy Threshold Analysis
for the
Enterprise Mission Enabling System (EMES)
NOAA8850

U.S. Department of Commerce Privacy Threshold Analysis

NWS Enterprise Mission Enabling System (EMES)

NOAA8850

Unique Project Identifier: 006-000351104 00-48-02-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

NOAA8850

The NWS Enterprise Mission Enabling System (EMES) is defined as a group of complementary enterprise services that provide a secure and reliable infrastructure throughout the NWS organization. EMES consists of Microsoft Active Directory (AD), McAfee ePolicy Orchestrator (ePO), Centralized Certificate Authority (CCA), and Enterprise Cybersecurity Monitoring and Operations (ECMO). Each of these separate products work together to provide authentication, security, reliability, inventory and an overall continuity of enterprise service for NWS staff. These tools ensure that only properly identified network devices connect to the NWS Network; run the latest software; run in a secure environment; and only properly identified and authorized NWS staff gain network access. The system employs redundancy to ensure reliability and availability while reducing latency and bandwidth.

NOAA8850 provides network infrastructure support, management, and connectivity services to the desktop and server customers within the NOAA8850 accreditation boundary, for administrative functions to include:

- Service Desk support,
- Active Directory (AD) services,
- File and print services
- File backup and restoration,
- Network Attached Storage (NAS)
- Dynamic Host Configuration Protocol (DHCP) and IP address space allocation
- Windows Internet Name Services (WINS)
- Domain Name Service (DNS),
- Application distribution and patch management,
- Backup and disaster recovery

In addition, it provides system-level support for servers, desktop computers/workstations, and laptops; and a test lab for systems and network engineers to develop and test new technologies, and to pre-configure new equipment for deployment. Lastly, the NOAA8850 AD user base receives electronic mail and calendar services from the NOAA Messaging Operations Center.

Microsoft Active Directory
Microsoft Active Directory is a special purpose database that authenticates and authorizes all users and computers in a Windows domain network. It is responsible for assigning and enforcing security policies for all computers. Active Directory checks the submitted password and authorizes user access to the system. Multiple Domain Controllers maintain copies of the AD Database and provide redundancy if another Domain Controller is unavailable. Domain Controllers are located in regional offices and key field offices to provide user access and reduce bandwidth.

McAfee ePolicy Orchestrator (ePO)
McAfee ePolicy Orchestrator is an integrated security software program designed to integrate the numerous security programs and to provide real time monitoring of security programs through a single console. McAfee EPO provides end-to-end visibility with a unified view of your security posture**,** simplified security operations, real-time security status, and an open architecture enabling faster response times.

Enterprise Cybersecurity Monitoring and Operations (ECMO)
U.S. Office of Management and Budget (OMB) memoranda M-10-15 and M-10-19 require all Federal agencies to continuously monitor security-related information from across the enterprise and present this information to the various levels of agency-wide management to enable timely decision making. The ECMO initiative will fulfill this requirement, providing essential, near real-time security status and remediation, increasing visibility into system operations and helping security personnel make risk-management decisions based on increased situational awareness. ECMO will also provide performance metrics to support the administration priority performance areas for continuous monitoring, automated asset management, automated configuration management, and automated vulnerability management.

Centralized Certificate Authority (CCA)
Centralized Certificate Authority issues certificates for day-to-day encryption needs, for encrypting local files and file systems, encrypting the communications between client workstation and servers, as well as server-to-server communication encryption. NOAA8850 utilizes 9 separate types of encryption for protecting information in transit and at rest. The nature of the encryption varies depending on the user need for access to the data, the sensitivity of the data, and the nature of the data being encrypted.

NOAA8850 also includes the National Weather Service Headquarters Local Area Network Infrastructure, which consists of domain controllers, servers, desktop/workstation, laptops, printers and network infrastructure components. The Infrastructure is located within the Silver Spring Metro Complex Building 2 (SSMC-2) and supports approximately 130 users and 380 network devices.

The network infrastructure team provides the support, management and connectivity services for administrative functions to include: Service Desk support, Active Directory, file and print, file backup and restoration, storage, Dynamic Host Configuration Protocol, Windows Internet Name Services, Domain Name Service, IP address space allocation, application distribution and patch management, backup and disaster recovery to the desktop and server customers within the accreditation boundary. In addition, it provides system-level support for servers, desktops/workstations, and laptops and a test lab mimicking the

production environment for systems and network engineers to develop and test new technologies. *All servers are located in the Silver Spring Metro Campus in Maryland.*

Multi Year Planning System (MYPS)
The Multi Year Planning System (MYPS) is comprised of three General Services Systems (GSS) and includes 20 servers (CFO1 servers). The GSS are the MYPS Labor Projection Model, Management Analysis and Reporting System Business Intelligence (BI) Maintenance Platform (MARS), and the General Forecaster Vacancy System. The Labor Projection Model and the General Forecaster Vacancy System are operational production systems. MARS BI Maintenance Platform is used only for maintenance efforts related to the production and pre-production MARS systems which are housed at the NOAA Information Technology Center.

The MYPS Labor Projection Model is a tool used to compute the multi-year total NWS labor five-year model using a detailed site-by-site, bottom-up cost approach. It calculates labor costs by site by position with the impact of changes in staffing levels. The model applies a labor lapse, calculates FTE, benefits, premium pay (shift differential), overtime, locality pay, COLA, special IT pay, awards, and annual pay raises. Costs are calculated using OPM-published salary and rates tables. All costs are categorized by ACCS, cost category, funding source, and portfolio. In addition, the model is used in "what-if" analyses to answer questions about proposed changes in labor such as lapse, labor rates, inflation, and table of organization changes. The resulting five-year answer sets are used to answer detailed questions about labor planning for NWS, NOAA, DOC, OMB, and Congressional requests. The labor data contained in the model's database is the master authorized (funded) position data for NWS.

MARS is a NOAA enterprise system that provides a common Business Intelligence platform to all NOAA Line Offices for financial reporting and querying, budget planning and commitment tracking. It consists of two modules, Reporting and Querying and Data Entry. The Data Entry module is not supported by MYPS. The MARS Reporting and Querying module is a business intelligence maintenance environment used for on-going design, creation and testing of new reports; new extract, transform and load (ETL) jobs; and software patches and upgrades for eventual deployment to the Reporting and Querying module of MARS.

The Radar Product Improvement System (RPI)
The Radar Product Improvement System (RPI) is defined as a testing and development platform for new functionality within Radar Product Generator (RPG), Supplemental Product Generator (SPG) and Advanced Weather Interactive Processing System (AWIPS). Its mission is to aide in the evolution of NOAA's NWS as an agile agency supporting emergency managers, first responders, government officials, businesses, and the public. The strategy is to improve the accuracy and usefulness of forecasts. To do so, RPI provides live radar data feeds from the Air Route Surveillance Radar System (ARSR-4) located in Guantanamo Bay, Cuba, and maintained by the Federal Aviation Administration (FAA). The ARSR-4 for RPI purposes, provides weather processing capabilities levied by RPI to generate Radar products for AWIPS testing. RPI ingests Level 2 radar data from ARSR-4 and generates Level 3 radar products. All data is categorized by FIPS 199 as "Environmental Monitoring and Forecasting".

RPI interfaces with the NWS Enterprise Mission Enabling System (NOAA8850) through the user access switch UA-SW-07103-0701 located at SSMC2. All RPI equipment is government owned and also located at SSMC2, Silver Spring MD.

The National AWIPS Program Office (NAPO)

The National AWIPS Program Office (NAPO) mission is to support activities related to the development of the Advanced Weather Interactive Processing System (AWIPS). Build Servers compile code and ingest live data to assist in the AWIPS process. As a development environment, NAPO provides: build machines for fabricating test Redhat Package Manager (RPMS) and a Network Attached Server (NAS) for backup storage and shared storage.

NAPO features the implementation of live data feeds which support a wide variety of development projects and configurations. The NAPO systems makes available to its developers a live NOAAport SBN feed and a feed from the Ground Segment, over which live weather satellites, GOES16 and GOES17, GOES rebroadcast (GBR) space packets are received.

Information sharing: Information is shared outside the bureau only if there has been a security breach.

NOAA8850 has a FIPS 199 moderate level rating.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) Whether it is a general support system, major application, or other type of system

General Support System (GSS)

b) System location

Silver Spring, MD

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

EMES have interconnections with other NWS NOAA FISMA IDs, Such as: NOAA8100- CBITS, NOAA8016-UAOS, NOAA8202-OWP, NOAA8203-N-PMS, NOAA8860-WCCIS, NOAA8872-MDLNet and all of NWS Region Headquarters (AR,CR,ER,PR,SR, WR)

d) The purpose that the system is designed to serve

EMES provide enterprise services and a reliable infrastructure throughout the NWS organization. Also, provides network infrastructure support, management, and connectivity services to the desktop and server customers within the NOAA8850 accreditation boundary, for administrative functions.

e) The way the system operates to achieve the purpose

The Multi Year Planning System (MYPS) is comprised of three General Services Systems (GSS) and includes 20 servers (CFO1 servers). The GSS are the MYPS Labor Projection Model, Management Analysis and Reporting System BI Maintenance Platform (MARS), and the General Forecaster Vacancy System. The Labor Projection Model and the General Forecaster Vacancy System are operational production systems. MARS BI Maintenance Platform is used only for maintenance efforts related to the production and pre-production MARS systems which are housed at the NOAA Information Technology Center.

The MYPS Labor Projection Model is a tool used to compute the multi-year total NWS labor five-year model using a detailed site-by-site, bottom-up cost approach. It calculates labor costs by site by position with the impact of changes in staffing levels. The model applies a labor lapse, calculates FTE, benefits, premium pay (shift differential), overtime, locality pay, COLA, special IT pay, awards, and annual pay raises. Costs are calculated using OPM-published salary and rates tables. All costs are categorized by ACCS, cost category, funding source, and portfolio. In addition, the model is used in "what-if" analyses to answer questions about proposed changes in labor such as lapse, labor rates, inflation, and table of organization changes. The resulting five-year answer sets are used to answer detailed questions about labor planning for NWS, NOAA, DOC, OMB, and Congressional requests. The labor data contained in the model's database is the master authorized (funded) position data for NWS.

MARS is a NOAA enterprise system that provides a common BI platform to all NOAA Line Offices for financial reporting and querying, budget planning and commitment tracking. It consists of two modules, Reporting and Querying and Data Entry. The Data Entry module is not supported by MYPS. The MARS Reporting and Querying module is a business intelligence maintenance environment used for on-going design, creation and testing of new reports; new extract, transform and load (ETL) jobs; and software patches and upgrades for eventual deployment to the Reporting and Querying module of MARS.

f) A general description of the type of information collected, maintained, use, or disseminated by the system

General Personal Data (Names, Gender, Age, Military Service, etc.)
Worked-Related Data (Occupation, Job Title , Salary, etc.)
System Administration/Audit Data (User ID, IP Address)

g) Identify individuals who have access to information on the system

DOC employees and contractors that are issued GFE's by DOC. All employees and contractors are issued CACs prior to accessing the system.

h) How information in the system is retrieved by the user

MYPS and MARS has its own user logon system and is accessed by its sole user and its maintenance support staff via the NOAA Silver Spring Metro Campus (SSMC) trusted campus network.

i) How information is transmitted to and from the system.

PII information is protected physically through the implementation of badged access to the information system and logically through Roble Based Access Controls. Data on laptops are encrypted at rest using AES-256. Sensitive Data, such as PII, is transmitted via Kiteworks using AES-256 encryption.

Information is shared outside the bureau only if there has been a security breach.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015). *Continue to answer questions and complete certification.*

_X_ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

_X_ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII.

_X_ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

_X_ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

_X_ DOC employees
_X_ National Institute of Standards and Technology Associates
_X_ Contractors working on behalf of DOC
____ Other Federal Government personnel
____ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

____ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.

Provide the legal authority which permits the collection of SSNs, including truncated form.

_X_ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

_X_ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

_X_ I certify the criteria implied by one or more of the questions above **apply** to the Enterprise Mission Enabling System and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the Enterprise Mission Enabling System and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Jeff Williams

Signature of SO: _____ Digitally signed by WILLIAMS.JEFFREY.D.1128972877 Date: 2020.07.22 07:30:52 -05'00' Date: _____

Name of Information Technology Security Officer (ITSO): Andrew Browne

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2020.07.22 09:12:39 -04'00' Date: _____

Name of Privacy Act Officer (PAO): Adrienne Thomas

Signature of PAO: THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2020.07.23 09:37:46 -04'00' Date: _____

Name of Authorizing Official (AO): Beckie Koonge

Signature of AO: KOONGE.BECKIE.A.1408306880 Digitally signed by KOONGE.BECKIE.A.1408306880 Date: 2020.07.22 16:01:57 -04'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2020.08.03 17:09:03 -04'00' Date: _____